UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/693,149	10/23/2003	Frederick S. M. Herz	REFH-0163	1678

23377 7590 08/31/2010
WOODCOCK WASHBURN LLP
CIRA CENTRE, 12TH FLOOR
2929 ARCH STREET
PHILADELPHIA, PA 19104-2891

EXAMINER	
WYSZYNSKI, AUBREY H	

ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
08/31/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/693,149	**Applicant(s)** HERZ, FREDERICK S. M.	
	Examiner AUBREY H. WYSZYNSKI	**Art Unit** 2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 July 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2,4-14 and 16-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2,4-14 and 16-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 7/2/10 has been entered.

2. The response of 5/3/10 was received and considered.

3. Claims 1, 3 and 15 have been canceled.

4. Claims 2, 4-14 and 16-21 are pending.

Response to Arguments

5. Applicant's arguments with respect to claims 2, 4-14 and 16-21 have been considered but are moot in view of the new ground(s) of rejection.

6. The added claim limitations are not adequate to place the claims in condition for allowance. In order to further expedite prosecution, applicant is encouraged to file detailed amendments. The applicant is encouraged to contact the examiner in the event that an interview may clarify or expedite any issues in the case.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 2, 4-14 and 16-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lin et al., US 6,405,250 and in further view of Anderson US 2003/0002436.

Regarding claims 2, 5, and 18, Lin discloses a system that detects the state of a computer network, comprising:

a plurality of distributed agents (fig. 1, NE management agents 111-114 and fig. 4, NE management agent 450) disposed in said computer network each said disturbed agent comprising:

data collection means for passively collecting, monitoring, and aggregating data representative of activities of respective nodes within said computer network (col. 3, lines 7-13, each management agent captures the behaviors of each corresponding network element NE 101-104 under its operating conditions and maintains a behavior transition model for its associated NE);

means responsive to the data from the data collection means for analyzing said data to develop activity models representative of activities of said computer network in a normal state and activities of said computer network in an abnormal state (col. 5, lines 1-13, using the behavior transition models for each NE, a network-wide behavior transition model can be constructed, the states of this network-wide model are composite states, the model has an initial state corresponding to a situation where all the NE's of the network are in their normal operating state, such as state 1 in Fig. 2 and col. 5, lines 30-44, wherein states 2 and 3 of fig. 2 represent BAD or “abnormal” states) Lin lacks or does not expressly disclose as a result of intrusions, infections, scams and/or other suspicious activities in said computer network.

However, Anderson states as a result of intrusions, infections, scams and/or other suspicious activities in said computer network (fig. 2, and ¶0026, Director collects data to determine the state of a network link and determines of network link is being abused or is the interest of suspicious behavior).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Lin with Anderson to determine if a state in the behavior transition models is based on suspicious behavior based on Anderson’s director to collect data of suspicious activity in order to determine if a network link is being misused, as taught by Anderson, ¶0026.

Lin, as modified above further discloses means for comparing collected data to said activity models to determine whether said computer network is in said normal state or said abnormal state at different times and to dynamically update said activity models based on said collected data (col. 5, lines 30-44, by monitoring the operating status of NE’s and traversing the transitions in the network-wide model, we can determine if certain deviations from all normal operating NE’s are good or bad and col. 6, lines 2-6, dynamically updating each NE based on network status),

wherein said analyzing means performs a pattern analysis on the collected data and said comparing means compares the results of the pattern analysis of data collected by an agent to the results of pattern analysis of data collected by analyzing means of other agents to identify similar patterns of suspicious activity in different portions of the computer network (col. 9, lines 1-15 and fig. 7, trend analyzer 402 compares newly received collected data to previous values and consults the behavior transition models to determine trends in the network, fig. 7, step 712 determine operating movement trends and step 713, identify potential future transitions).

Regarding claim 4, Lin as modified above discloses the system of claim 2, wherein said data collection means collects data representative of operation of said computer network, including respective nodes in said computer network, said data relating to communications, internal and external accesses, code execution functions, and/or network resource conditions of respective nodes in said computer network (col. 3, lines 7-14, creation of a behavior transition model for capturing the behaviors of each NE 101-104 under the influence of operating conditions in its internal and external environments.).

Regarding claim 6, Lin as modified above discloses the system of claim 2, further comprising means for characterizing the state of the computer network and identifying any potential threats based on said collected data (figs. 2 and 3, composite states. Also, Anderson, fig. 2, step 206, detect if network link is being misused).

Regarding claim 7, Lin as modified above discloses the system of claim 6, wherein said characterizing means further recommends remedial repair and/or recovery strategies to isolate and/or neutralize the identified potential threats to the computer system (fig. 7, and fig. 4, action chooser 403. Also, Anderson, fig. 2, steps 214-218, determines regulation).

Regarding claim 8, Lin as modified above discloses the system of claim 2, wherein respective agents are connected by redundant communications connections (fig. 1. Also, Anderson, fig. 1, sensors 104 and routing devices 106).

Regarding claim 9, Lin as modified above discloses the system of claim 2, wherein each agent is implemented in redundant memory and hardware that is adapted to be insulated from infected components of said computer network (Anderson, fig. 5, step 510).

Regarding claim 10, Lin as modified above discloses the system of claim 2, wherein the agents are disposed in a hierarchical structure whereby communications from bottom level agents to agents at higher levels in the hierarchy are limited (col. 7, lines 1-6).

Regarding claim 11, Lin as modified above discloses the system of claim 2, further comprising means for predictively modeling the behavior of said computer network based on sequentially occurring behavior patterns in the data collected by said data collection means (fig. 7, step 713, identify potential future transitions).

Regarding claim 12, Lin as modified above discloses the system of claim 2 wherein said comparing means comprises means for pattern matching collected data with data in said activity models to determine a closest activity model based upon similarity of the data in each data model with the collected data (fig. 7, step 712, determine operating point movement trend).

Regarding claim 13, Lin as modified above discloses the system of claim 2, wherein the collected data represents actions of a virus, system responses to actions of a virus, actions of a hacker, system responses to actions of a hacker, threats directed to discrete objects in said computer network, and/or potential triggers of a virus or threat to said computer network (Anderson, ¶0032, network misuse).

Regarding claim 14, Lin as modified above discloses the system of claim 2, wherein said analyzing means for each agent filters and analyzes received data and dynamically redistributes the analyzed and filtered data to other agents associated with said each agent (col. 6, lines 2-11).

Regarding claim 16, Lin as modified above discloses the system of claim 2, wherein the comparing means compares names and email addresses in said collected data against known criminal, hoaxsters and/or aliases for known criminals and hoaxsters (Anderson, ¶0005).

Regarding claim 17, Lin as modified above discloses the system of claim 2, further comprising a trusted server that receives attack data from a plurality of agents identifying abnormal states indicative of a network attack, said trusted server gathering the attack data and sending warnings to selected nodes in said computer network (Anderson, fig. 6, alert).

Regarding claim 19, Lin as modified above discloses the method of claim 18, wherein the agents report any suspicious activity that exceeds a suspicion threshold (Anderson, ¶0032, user define threshold).

Regarding claim 20, Lin as modified above discloses the method of claim 19, wherein the agents transmit said analyzed data in order to determine an origin of the suspicious activity in the computer network (Anderson, ¶0032).

Regarding claim 21, Lin as modified above discloses the method of claim 20, further comprising scanning said analyzed data for patterns and comparing said patterns to data representative of patterns of known threats to said computer network for identification of said suspicious activity (¶fig. 7, steps 712-713).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AUBREY H. WYSZYNSKI whose telephone number is (571)272-8155. The examiner can normally be reached on Monday - Thursday, and alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571)272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aubrey H Wyszynski/
Examiner, Art Unit 2434
/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434